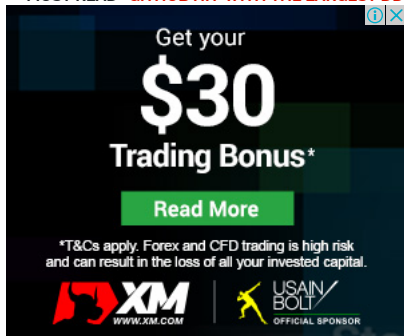


MUST READ **GITHUB HIT WITH THE LARGEST DDOS ATTACK EVER SEEN**


Get your
\$30
Trading Bonus*

Read More

*T&Cs apply. Forex and CFD trading is high risk and can result in the loss of all your invested capital.

XM
WWW.XM.COM

USAIN BOLT
OFFICIAL SPONSOR

in: High-profile cryptocurrency catastrophes of 2017

team acceptance, ZDNet reviews the high-profile disasters, data breaches, vulnerabilities, digital currency in 2017.

ber 13, 2017 -- 15:40 GMT (23:40 GMT+08:00) | Topic: [2017: The Year's Best Tech for Work and Play](#)



Skip Ad

Ad: (6:23)

-
- playlist

Video: Why rising bitcoin prices are not all good news for ransomware writers

In the last few months, the cryptocurrency industry has exploded with investor interest appearing to be at an all-time high.

The price of Bitcoin alone has surged thousands of dollars in the past few weeks, topping \$16,500 [at the time of writing](https://www.coindesk.com/price/) (<https://www.coindesk.com/price/>), and while some investors plea caution and anticipate a crash, the rise has highlighted just how much interest there is in digital coins and alternative payment methods.

Over the course of the past year, traditional financial institutions have begun exploring cryptocurrency and its backbone infrastructure, digital ledger technologies known as blockchain, with some banks going so far as to offer their clients [cryptocurrency-supporting trading accounts](http://www.zdnet.com/article/falcon-bank-offers-clients-cryptocurrency-trades/) (<http://www.zdnet.com/article/falcon-bank-offers-clients-cryptocurrency-trades/>) and options.

This month, Venezuelan President Nicolas Maduro went as far as to announce a plan to create "Petro," a [sovereign virtual currency](http://www.zdnet.com/article/venezuelas-petro-cryptocurrency-tipped-as-way-out-of-economic-crisis/) (<http://www.zdnet.com/article/venezuelas-petro-cryptocurrency-tipped-as-way-out-of-economic-crisis/>) which he claims can be used to help dig the country out of its current economic crisis.

MORE SECURITY NEWS

New LTE attacks can snoop on messages, track locations and spoof emergency alerts
(<http://www.zdnet.com/article/new-lte-attacks-eavesdrop-on-messages-track-locations-spoof-alerts/>)

Microsoft: Windows Defender can now spot FinFisher government spyware
(<http://www.zdnet.com/article/microsoft-windows-defender-can-now-spot-finfisher-government-spyware/>)

Hacking operation uses malicious Word documents to target aid organisations
(<http://www.zdnet.com/article/hacking-operation-uses-malicious-word-documents-to-target-aid-organisations/>)

On TechRepublic: [18 new IT jobs created by Bitcoin and blockchain](https://www.techrepublic.com/article/18-new-it-jobs-created-by-bitcoin-and-blockchain/) (<https://www.techrepublic.com/article/18-new-it-jobs-created-by-bitcoin-and-blockchain/>) (<http://www.zdnet.com/article/executives-guide-to-blockchain/>)

Signal, Telegram users experience outages worldwide (<http://www.zdnet.com/article/signal-telegram-users-experience-outages-worldwide/>)

Get your
\$30
Trading Bonus*

Read More

*T&Cs apply. Forex and CFD trading is high risk and can result in the loss of all your invested capital.

XM
www.xm.com

USA IN BOLT
OFFICIAL SPONSOR

have its benefits. The [blockchain has garnered interest in the](http://www.zdnet.com/article/executives-guide-to-blockchain/) and beyond as a secure method to -- with IBM one of many now offering [blockchain-based business](#) while cryptocurrency, when bought early, has proved to be a lucrative investment. up and smash investor dreams to pieces.

[United Kingdom plans tighter regulation of bitcoin](http://www.zdnet.com/article/united-kingdom-plans-tighter-regulation-of-bitcoin/) and [US](http://www.zdnet.com/article/us-decrees-ethereum) (<http://www.zdnet.com/article/us-decrees-ethereum>) [hoping to control this industry](#), of which many investors are [failing to declare cryptocurrency profits](#) [coinbase-user-records-of-bitcoin-transactions/](#)), but on the other side of the spectrum, some are losing cash due to poorly managed Initial Coin Offerings (ICOs), vulnerabilities, malware, and more.

See also: [Bitcoin futures begin trading](http://www.zdnet.com/article/bitcoin-futures-begin-trading/) (<http://www.zdnet.com/article/bitcoin-futures-begin-trading/>) | [Ransomware's bitcoin problem: How price surge means a headache for crooks](http://www.zdnet.com/article/ransomwares-bitcoin-problem-how-price-surge-means-a-headache-for-crooks/) (<http://www.zdnet.com/article/ransomwares-bitcoin-problem-how-price-surge-means-a-headache-for-crooks/>) | [JPMorgan calls Bitcoin 'fraud' only for use by criminals and North Koreans](http://www.zdnet.com/article/jp-morgan-calls-bitcoin-fraud-only-useful-for-criminals-and-north-koreans/) (<http://www.zdnet.com/article/jp-morgan-calls-bitcoin-fraud-only-useful-for-criminals-and-north-koreans/>) | [TechRepublic: Why more companies will be betting on Bitcoin in 2018](https://www.techrepublic.com/article/why-more-companies-will-be-betting-on-bitcoin-in-2018/) (<https://www.techrepublic.com/article/why-more-companies-will-be-betting-on-bitcoin-in-2018/>)

It was back in 2014 with the [abrupt closure of Bitcoin trading platform](http://www.zdnet.com/article/russian-bitcoin-exchange-chief-arrested-in-connection-to-mt-gox-hack/) (<http://www.zdnet.com/article/russian-bitcoin-exchange-chief-arrested-in-connection-to-mt-gox-hack/>) Mt. Gox which signaled all may not be well in the industry when it came to security. Investors are highly unlikely to ever get their money back and the former CEO, Mark Karpeles, faces charges of embezzlement.

Since then, cryptocurrency interest has increased, but so has the security issues surrounding investment.

2017 was an interesting year for the industry, with hacks, vulnerabilities, and data breaches a constant theme.

January was a quiet month as we all recovered from the holiday season, but in **February**, programmers were left shamefaced after a simple typing error caused the loss of Zcoins worth \$585,000 at the time.

[According to Zcoin](https://thehackernews.com/2017/02/zcoin-zerocoin-typo.html) (<https://thehackernews.com/2017/02/zcoin-zerocoin-typo.html>), a "typographical error on a single additional character" in the Zerocoin source code allowed an attacker to generate additional Zcoins during a single transaction, leading to the theft of roughly 370,000 Zcoins.

Little of note took place in **March**, but in **April**, OneCoin representatives were in the middle of a sales pitch related to cryptocurrency when law enforcement [raided the company](https://timesofindia.indiatimes.com/city/navi-mumbai/e-currency-racket-rs-19-crore-seized-from-bank-a/cs-in-delhi-raj/articleshow/58388071.cms) (<https://timesofindia.indiatimes.com/city/navi-mumbai/e-currency-racket-rs-19-crore-seized-from-bank-a/cs-in-delhi-raj/articleshow/58388071.cms>), jailing 18 employees and freezing roughly \$2 million in investor funds.

Local Delhi police said the company only accepted cash for cryptocurrency and did not issue receipts in order to cover its tracks, therefore suggesting the entire scheme was a scam. (However, this is not to be confused with the China-based Xunlei's [OneCoin](https://qz.com/1152564/the-hottest-cryptocurrency-in-china-isnt-bitcoin-its-onecoin-make-that-lianke-by-xunlei-xnet/) (<https://qz.com/1152564/the-hottest-cryptocurrency-in-china-isnt-bitcoin-its-onecoin-make-that-lianke-by-xunlei-xnet/>)).

Little of note happened in **May**, but in **June**, the US Securities and Exchange Commission (SEC) [won a court case](http://www.zdnet.com/article/bitcoin-scam-firms-slammed-with-12-million-penalty/) (<http://www.zdnet.com/article/bitcoin-scam-firms-slammed-with-12-million-penalty/>) against the now-defunct GAW Miners and Zen Miners, both of which were accused of running Bitcoin Ponzi schemes which defrauded investors with "the lure of quick riches from virtual currency."

These were 2017's biggest hacks, leaks, and... (</pictures/biggest-hacks-leaks-and-data-breaches-2017/>)

SEE FULL GALLERY (</pictures/biggest-hacks-leaks-and-data-breaches-2017/>)

SPECIAL REPORT

(<http://www.techrepublic.com/resource-library/whitepapers/the-executive-guide-to-implementing-blockchain-technology/>)

Download the Blockchain Guide (<http://www.techrepublic.com/resource-library/whitepapers/the-executive-guide-to-implementing-blockchain-technology/>)

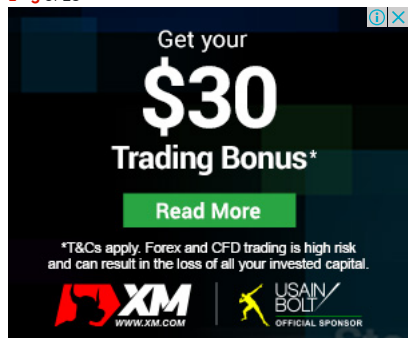
You can read this executive guide as a PDF (free registration required).

Read More (<http://www.techrepublic.com/resource-library/whitepapers/the-executive-guide-to-implementing-blockchain-technology/>)



1 - 5 of 28

NEXT > 0



targeted for investor funds and cyberattackers running amok.

hackers used a disarmingly simple tactic to capitalize on investor enthusiasm and [steal roughly \\$7.4 million](#) [in-ethereum-during-coindash-ico-launch/](#) in Ethereum (ETH).

used the CoinDash website and simply changed a wallet address intended for investors during the ICO to a

ized what had occurred, but the damage was done.

Just a week after, Veritaseum's ICO [met a similar fate](#) (<https://www.coindesk.com/veritaseum-founder-claims-8-million-ico-token-stolen/>). In total, 36,000 VERI tokens were stolen by hackers during the event, worth nearly \$8 million at the time. The tokens, however, belonged to the company and not investors.

South Korean exchange Bithumb, the fourth largest exchange worldwide, also became a victim in July as thieves managed to [steal a database of user information](#) (<https://thehackernews.com/2017/07/bitcoin-ethereum-cryptocurrency-exchange.html>) from an employee's personal PC to compromise user accounts, resulting in the theft of information and Bitcoin worth billions of won.

In the same month, the Parity wallet was compromised by an attacker who slinked away with [over \\$30 million](#) (<http://www.zdnet.com/article/hackers-strike-ethereum-again-slink-away-with-over-30-million/>) in Ethereum.

At least three wallets were compromised through the exploit of a vulnerability in the wallet, with Edgeless Casino, Aeternity, and Swarm City named as victims.

To prevent more wallets being drained, white hats took charge and drained user wallets themselves to hold them until the bug was fixed.

In **August**, hackers used a simple trick to swindle investors on the Ethereum platform Enigma.

As the marketplace was gearing up for its ICO, potential traders were sent "very convincing" emails announcing a "pre-sale" of tokens and inviting them to participate.

While some users recognized the emails as a scam, others did not, parting with close to [\\$500,000 in Ethereum](#) (<http://www.zdnet.com/article/enigma-ethereum-marketplace-hijacked-by-attackers/>). It appears that the user details were gained through the compromise of the Enigma Slack channel and email lists.

In **September**, the US Commodity Futures Trading Commission (CFTC) [filed a court case](#) (<http://www.cftc.gov/PressRoom/PressReleases/pr7614-17>) against Nicholas Gelfman and Gelfman Blueprint, alleging that the company scammed roughly 80 investors out of \$600,000 through a Ponzi scheme.

The victims were reportedly actually involved in an exit scheme and were told the "Jigsaw" trading platform had been hacked.

o, [by outlawing ICOs](#) (<http://www.zdnet.com/article/south-korea-bans-digital-currency-offerings/>) due to the risk of

Subscribe to our
Innovations Weekly
newsletter

Email Address

☐ I agree to the Terms of Use, Privacy Policy and Video Services Policy. I understand I will receive a complimentary subscription to ZDNet's Tech Today newsletter, and the ZDNet Announce newsletter (you can opt out at any time).

SUBSCRIBE

[m/article/bitcoin-launderer-suspect-caught-in-us-russia-extradition-spat/](#)) became the source of a fight between the [e him with suspected Bitcoin laundering](#). The Russian national allegedly was the mastermind behind [customer information, allowing for laundering to take place](#).

[ily shut down](#) (<https://medium.com/etherparty/etherparty-thwarts-site-attack-on-successful-ico-launch-day-company-will-sale-after-45-minutes-into-the-event-in-the-same-month-after-a-cyberattacker-switched-the-firm-s-wallet>

address with one they owned in an attempt to steal user funds.

Impacted investors were compensated.

Perhaps due to the risks some ICOs represented to investors, China took the same stance as South Korea, [banning ICOs](http://www.zdnet.com/article/china-banning-icos/) (<http://www.zdnet.com/article/china-banning-icos/>) in the same month.



er, a start-up used to exchange cryptocurrency backed by traditional cash. The company [revealed](#) that cybercriminals managed to compromise its treasury wallet and steal \$30,950,010 USDT -- a token linked to an unauthorized wallet.

to recover the lost funds.

currency space. An Ethereum user, poking around the Parity wallet -- used to store and trade Ethereum -- <http://www.zdnet.com/article/ethereum-user-accidentally-exploits-major-vulnerability-locks-wallets/> hidden within the library of the standard multi-sig contract.

The user was able to make himself an owner of a contract and at the same time wiped out a critical element of library code which locked other users out of their wallets.

The actions of the user resulted in \$160 million in funds being frozen.

A solution is [yet to be found](http://www.zdnet.com/article/parity-shakes-up-wallet-audits-but-funds-remain-frozen/) (<http://www.zdnet.com/article/parity-shakes-up-wallet-audits-but-funds-remain-frozen/>), although a [hard fork](https://www.coindesk.com/parity-proposes-hard-fork-to-reclaim-frozen-160-million/) (<https://www.coindesk.com/parity-proposes-hard-fork-to-reclaim-frozen-160-million/>) has been proposed as a potential solution.

While companies grappled with the aftermath of theft and data breaches, a 47-year-old pastor in New Jersey was [sentenced to over five years](https://www.ethnews.com/prison-for-pastor-trevon-gross-in-coin-mx-case) (<https://www.ethnews.com/prison-for-pastor-trevon-gross-in-coin-mx-case>) in prison for accepting bribes through the unlicensed, illegal Coin.mx Bitcoin exchange through his community church.

It may be the season for holiday cheer, but few NiceHash users are going to have a good season. In **December**, [the company admitted](http://www.zdnet.com/article/bitcoin-exchange-nicehash-hacked-70m-lost/) (<http://www.zdnet.com/article/bitcoin-exchange-nicehash-hacked-70m-lost/>) that \$68 million in investor funds had been stolen from the NiceHash wallet, resulting in suspended operations. The full extent of the breach is still not yet known.

SEC took on another cryptocurrency outfit [in the same month](http://www.zdnet.com/article/sec-cyber-unit-files-charges-over-ico-fraud/) (<http://www.zdnet.com/article/sec-cyber-unit-files-charges-over-ico-fraud/>), filing charges against PlexCorps for allegedly conducting ICO fraud. The company raised up to \$15 million by promising investors a 13-fold profit within weeks.

Read more: [Quant Trojan upgrade targets Bitcoin, cryptocurrency wallets](http://www.zdnet.com/article/quant-trojan-upgrade-targets-cryptocurrency-user-wallets/) (<http://www.zdnet.com/article/quant-trojan-upgrade-targets-cryptocurrency-user-wallets/>)

Data breaches and successful hacks are not the only concerns in the cryptocurrency industry, however, with some threat actors embracing new variants of malware to steal user funds and compromise wallets.

While [reports suggest](https://qz.com/1110419/north-korea-may-be-using-malware-to-secretly-mine-ethereum-monero-or-zcash/) (<https://qz.com/1110419/north-korea-may-be-using-malware-to-secretly-mine-ethereum-monero-or-zcash/>) North Korea is secretly using malware to enslave PCs for the purposes of cryptocurrency mining, the concept was also brought closer to home this year.

Users of The Pirate Bay [reported CPU problems](http://www.zdnet.com/article/500-million-pcs-are-being-used-for-stealth-cryptocurrency-mining-online/) (<http://www.zdnet.com/article/500-million-pcs-are-being-used-for-stealth-cryptocurrency-mining-online/>) in October when visiting the torrent search website, which was later revealed to be due to a Monero mining pilot, implemented without user consent.

See also: [500 million PCs are being used for stealth cryptocurrency mining online](http://www.zdnet.com/article/500-million-pcs-are-being-used-for-stealth-cryptocurrency-mining-online/) (<http://www.zdnet.com/article/500-million-pcs-are-being-used-for-stealth-cryptocurrency-mining-online/>) | [Hackers hijack Coinhive cryptocurrency miner through an old password](http://www.zdnet.com/article/hackers-hijack-coinhive-dns-server-through-an-old-password/) (<http://www.zdnet.com/article/hackers-hijack-coinhive-dns-server-through-an-old-password/>) | [How much does The Pirate Bay's cryptocurrency miner make?](http://www.zdnet.com/article/how-much-does-the-pirate-bays-cryptocurrency-miner-make/) (<http://www.zdnet.com/article/how-much-does-the-pirate-bays-cryptocurrency-miner-make/>) | [Android security: Coin miners show up in apps and sites to wear out your CPU](http://www.zdnet.com/article/android-security-coin-miners-show-up-in-apps-and-sites-to-wear-out-your-cpu/) (<http://www.zdnet.com/article/android-security-coin-miners-show-up-in-apps-and-sites-to-wear-out-your-cpu/>)

Cloudflare is now blocking websites which use such software without user permission, and while lending CPU power in return for ad-free browsing may be a possible future, consent is key.

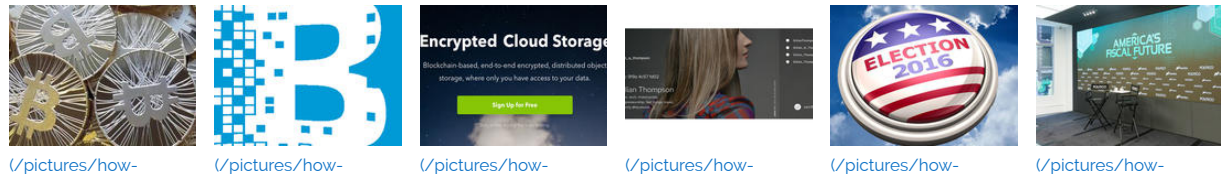
In the meantime, [Trend Micro says](http://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/) (<http://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/>) that Google Play is littered with mining apps masquerading as legitimate software.

But consumers who hold cryptocurrency, botnets, and malware designed to infiltrate wallets stored offline on user PCs are [also a growing threat](#) ([scams-beware-of-crooks-trying-to-steal-your-cryptocurrency-with-these-schemes/](#)).

The growing popularity of cryptocurrency and growing interest of attackers keen to cash in through malware, phishing, and attacking trader wallets have made users be careful.

While the future of cryptocurrency is uncertain, and investment, but cybersecurity will remain a challenge in 2018.

Learn more about how blockchain technology can transform our world... ([pictures/how-blockchain-technology-can-transform-our-world/](#))



1 - 5 of 6

NEXT > 0

PREVIOUS AND RELATED COVERAGE

[500 million PCs are being used for stealth cryptocurrency mining online](#) (<http://www.zdnet.com/article/500-million-pcs-are-being-used-for-stealth-cryptocurrency-mining-online/>)

Your PC may be used to find cryptocurrency when you visit websites, with or without your consent.

[Hackers hijack Coinhive cryptocurrency miner through an old password](#) (<http://www.zdnet.com/article/hackers-hijack-coinhive-dns-server-through-an-old-password/>)

Yet another lesson in how not to secure your network.

[Falcon bank offers clients Bitcoin, cryptocurrency trade accounts](#) (<http://www.zdnet.com/article/falcon-bank-offers-clients-cryptocurrency-trades/>)

Banking customers will now be able to hold and buy Bitcoin, but what does this mean for anonymity?

RELATED TOPICS:

BANKING

SECURITY TV

DATA MANAGEMENT

CXO

DATA CENTERS

Recommended For You

Sponsored Links by Taboola

Flight Prices You're Not Allowed to See!
Save70.com

Play this Game for 1 Minute and see why everyone is addicted
Delta Wars

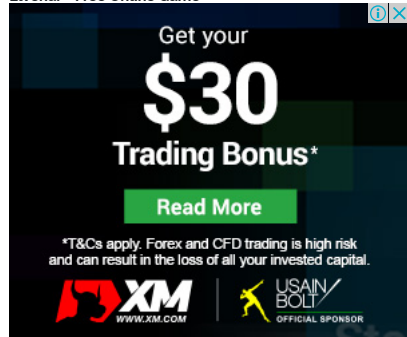
An Easy Way to Generate Some Extra Income
Survey Compare

10 Mom-Inspired Looks Fashion Girls Can't Stop Wearing
BleuBloom.com

Want To Be Own Boss In 2017? Start An Online Business In Your Spare Time!

Enter a Magical World in this Fantasy City Builder

Elvenar - Free Online Game



Fly

[Log in to comment](#) | [Community guidelines](#)

Join Discussion

ZDNet Comment Policy

Do not post advertisements, offensive material, profanity, or personal attacks. Please be considerate of others.
Please read our [Comment Policy](#) before commenting.



3 Comments

Share

Sort by Oldest ▾

**belairsummer** • 2 months ago

ranking ok
Share ›

**Lego125354** • a month ago

this article: "Here's how you can still get a free Windows 10 upgrade" is great - i just have one question: I have windows 8.1 retail box - i have upgraded to windows 10 pro - via the Microsoft offer - now what? if my computer will fail - hardware failure - i can only install windows 8.1? how can i "fix" my new situation as windows 10 pro owner?
Share ›

**exonym** • 6 days ago

Be careful !!!

Since 2018 Mega has a different goal. For 3 months 35 GB free or 20 GB free with MegaSync. After 3 months the account can only hold 15 GB
Share ›

ALSO ON ZDNET

Samsung Galaxy S9 Plus first impressions: Improving upon the S8 Plus just where it was ...

4 comments • 17 hours ago

frgough — And takes pictures (the best camera for taking pictures is the one you have with you at the time), and takes movies, and lets you browse the ...

Cheaper MacBook Air coming later this year, claims report

10 comments • 2 days ago

knuthf — Most of us do not accept the wasted time on insecure devices, and that renders two alternatives: Apple with MacBooks and PC that ...

iPhone, iPad, Mac? Here's how long your Apple device will last

31 comments • 18 hours ago

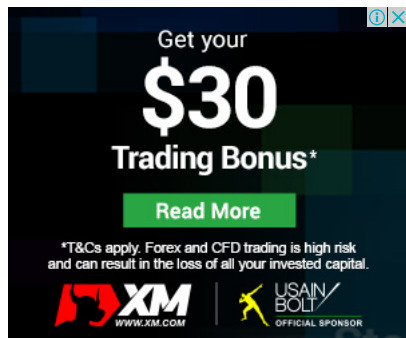
danixdefcon5 — I really dislike the anti-consumer trend in Apple; their pre-Retina MBPs were user serviceable to the degree required for serious ...

Amazon considers launching branded checking accounts for unbanked

14 hours ago

Genghis Hound — In a few years Amazon will announce its own money.

Privacy

[ADD YOUR COMMENT](#)

Get your
\$30
Trading Bonus*

[Read More](#)

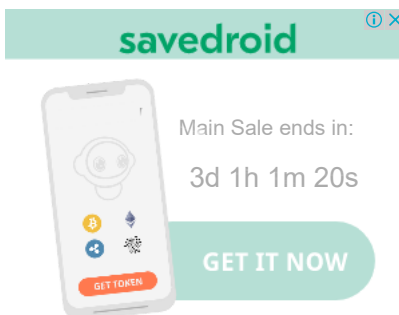
*T&Cs apply. Forex and CFD trading is high risk and can result in the loss of all your invested capital.

XM
www.xm.com

USAIN BOLT
OFFICIAL SPONSOR

SPONSORED

- 5 AVG Free Download
- 6 Block Chain
- 7 Free Antivirus Software
- 8 Quality Hearing Aids



savedroid

Main Sale ends in:
3d 1h 1m 20s

[GET IT NOW](#)



Dorado
Meet the next "UBER" on blockchain for deliveries

----- GET YOUR -----
30% BONUS

[Buy tokens](#)
[get 30% bonus](#)

10 things in cybersecurity that you might have missed in 2017

From frustrating to mysterious to downright creepy, here are ten things we learned during 2017.



By [Zack Whittaker](#) for [Zero Day](#) | January 2, 2018 -- 12:06 GMT (20:06 GMT+08:00) | Topic: [2017: The Year's Best Tech for Work and Play](#)

Video: Looking back on 2017

Thought you caught everything in security this year? There was a lot to unpack. Here are ten things we learned this year that you might have missed.

1. APPS CAN USE ULTRASONIC SOUNDS TO TRACK WHERE ITS USERS GO ([HTTP://WWW.ZDNET.COM/ARTICLE/HUNDREDS-OF-APPS-ARE-USING-ULTRASONIC-SOUNDS-TO-TRACK-YOUR-AD-HABITS/](http://www.zdnet.com/article/hundreds-of-apps-are-using-ultrasonic-sounds-to-track-your-ad-habits/))

These near-silent tones can't be picked up by the human ear, but there are apps in your phone that are always listening for them -- and can be used to build up a profile about what you've seen, where, and in some cases even the websites you've visited.

2. FACEBOOK CAN MATCH YOU WITH RELATIVES YOU DIDN'T EVEN KNOW YOU HAD ([HTTP://GIZMODO.COM/FACEBOOK-FIGURED-OUT-MY-FAMILY-SECRETS-AND-IT-WONT-TEL-1797696163](http://gizmodo.com/facebook-figured-out-my-family-secrets-and-it-wont-tel-1797696163))

A Gizmodo reporter discovered that Facebook had [suggested a long-lost relative](http://gizmodo.com/facebook-figured-out-my-family-secrets-and-it-wont-tel-1797696163) (<http://gizmodo.com/facebook-figured-out-my-family-secrets-and-it-wont-tel-1797696163>) through "People You May Know," a secret algorithmic feature on the site - even though they'd had no friends in common or an obvious connection of any kind. The social media giant wouldn't say how it put the two relatives together. File under "extremely creepy."

3. RANSOMWARE CAN STILL RUN ON WINDOWS 10 VERSIONS PROTECTED FROM RANSOMWARE ([HTTP://WWW.ZDNET.COM/ARTICLE/MICROSOFT-NO-KNOWN-RANSOMWARE-WINDOWS-WE-TRIED-TO-HACK-IT/](http://www.zdnet.com/article/microsoft-no-known-ransomware-windows-we-tried-to-hack-it/))

Microsoft said "no known ransomware" works on Windows 10 S, a locked down version that only allows apps through the Windows app store. We wanted to see if such a bold claim could hold up. ([It didn't](http://www.zdnet.com/article/microsoft-no-known-ransomware-windows-we-tried-to-hack-it/) (<http://www.zdnet.com/article/microsoft-no-known-ransomware-windows-we-tried-to-hack-it/>).

4. APPLE HIDES JOB POSTINGS ON SECRET SERVERS ([HTTP://WWW.ZDNET.COM/ARTICLE/HOW-WE-FOUND-THAT-HIDDEN-APPLE-JOB-POSTING/](http://www.zdnet.com/article/how-we-found-that-hidden-apple-job-posting/))

Apple hid a secret job posting on a [public-facing but hidden iCloud server](http://www.zdnet.com/article/how-we-found-that-hidden-apple-job-posting/) (<http://www.zdnet.com/article/how-we-found-that-hidden-apple-job-posting/>) earlier this year calling for a "a talented engineer to develop a critical infrastructure component that is to be a key part of the Apple ecosystem." Other companies also hide job postings in their website's source code and other unconventional places in an effort to try to appeal to the brightest and sharpest minds.

5. YOU CAN GET SUBPOENAED BY SIMPLY BEING MENTIONED IN A TWEET ([HTTPS://WWW.TECHDIRT.COM/ARTICLES/20171025/11290738482/DOJS-BIZARRE-SUBPOENA-OVER-EMOJI-HIGHLIGHTS-RIDICULOUS-VENDETTA-AGAINST-SECURITY-RESEARCHER.SHTML](https://www.techdirt.com/articles/20171025/11290738482/dojs-bizarre-subpoena-over-emoji-highlights-ridiculous-vendetta-against-security-researcher.shtml))

Five people, including a [respected data breach reporter](https://twitter.com/pogowasright) (<https://twitter.com/pogowasright>) and [renown lawyer and blogger](https://twitter.com/Popehat) (<https://twitter.com/Popehat>), were subpoenaed by the Justice Dept. for [simply being named in a tweet](https://www.techdirt.com/articles/20171023/18275838465/doj-subpoenas-twitter-about-popehat-dissent-doe-others-over-smiley-emoji-tweet.shtml) (<https://www.techdirt.com/articles/20171023/18275838465/doj-subpoenas-twitter-about-popehat-dissent-doe-others-over-smiley-emoji-tweet.shtml>). Prosecutors wanted a ton of information, including names, postal and IP addresses, and more in relation to a case that critics called a "vendetta" (<https://www.techdirt.com/articles/20171025/11290738482/dojs-bizarre-subpoena-over-emoji-highlights-ridiculous-vendetta-against-security-researcher.shtml>) against a security researcher.

YEAR IN REVIEW



(<http://www.zdnet.com/article/techs-leaps-limps-and-likes-the-7-trends-that-defined-2017/>)

Tech's leaps, limps and likes: The 7 trends that defined 2017
(<http://www.zdnet.com/article/techs-leaps-limps-and-likes-the-7-trends-that-defined-2017/>)

ZDNet's top editors from across the globe postulate on a year that the technology industry lost some luster, but kept rolling out new disruptions anyway.

Read More
(<http://www.zdnet.com/article/techs-leaps-limps-and-likes-the-7-trends-that-defined-2017/>)

6. MASS SURVEILLANCE MAY NOT ACTUALLY WORK ([HTTP://WWW.ZDNET.COM/ARTICLE/UN-PRIVACY-RAPPORTEUR-SAYS-LITTLE-OR-NO-EVIDENCE-THAT-SURVEILLANCE-LAWS-WORK/](http://www.zdnet.com/article/un-privacy-rapporteur-says-little-or-no-evidence-that-surveillance-laws-work/))

That's according to the United Nations' special rapporteur on privacy, who [earlier this year](http://www.zdnet.com/article/un-privacy-rapporteur-says-little-or-no-evidence-that-surveillance-laws-work/) (<http://www.zdnet.com/article/un-privacy-rapporteur-says-little-or-no-evidence-that-surveillance-laws-work/>) lambasted a spate of new surveillance laws across Europe and the US, saying there is "little to no evidence" that the mass monitoring of communication prevents terrorism.

7. NSA'S SPY PROGRAMS WON'T SWITCH OFF WHEN US' SPY LAW EXPIRES

([HTTPS://WWW.NYTIMES.COM/2017/12/06/US/POLITICS/WARRANTLESS-SURVEILLANCE-LEGISLATION-SECTION-702.HTML?_R=0](https://www.nytimes.com/2017/12/06/us/politics/warrantless-surveillance-legislation-section-702.html?_r=0))

A key law that allows the NSA to spy on foreigners overseas (and [many Americans](http://www.zdnet.com/article/us-violated-spy-laws-hundreds-of-times-in-the-past-decade/) (<http://www.zdnet.com/article/us-violated-spy-laws-hundreds-of-times-in-the-past-decade/>)) will expire at midnight on December 31, but because of how the surveillance programs are authorized, the legal power will roll over [until about April](https://www.nytimes.com/2017/12/06/us/politics/warrantless-surveillance-legislation-section-702.html?_r=0) (https://www.nytimes.com/2017/12/06/us/politics/warrantless-surveillance-legislation-section-702.html?_r=0). That gives Congress a few more months to sign a bill [to reform or reauthorize](http://www.zdnet.com/article/congress-mulls-nsa-surveillance-reform-the-good-bad-and-ugly-options/) (<http://www.zdnet.com/article/congress-mulls-nsa-surveillance-reform-the-good-bad-and-ugly-options/>) the nation's spy laws for the first time since the Edward Snowden disclosures.

8. DELETING YOUR YAHOO EMAIL ACCOUNT CAN BE SURPRISINGLY DIFFICULT ([HTTP://WWW.ZDNET.COM/ARTICLE/YAHOO-NOT-DELETING-EMAIL-ACCOUNTS-SAY-USERS/](http://www.zdnet.com/article/yahoo-not-deleting-email-accounts-say-users/))

After the massive 500 million account breach at Yahoo (the first of many -- the number [went up](http://www.zdnet.com/article/yahoo-hacked-again-more-than-one-billion-accounts-stolen/) (<http://www.zdnet.com/article/yahoo-hacked-again-more-than-one-billion-accounts-stolen/>) and [up again](http://www.zdnet.com/article/yahoo-believes-3-billion-affected-by-2013-hack/) (<http://www.zdnet.com/article/yahoo-believes-3-billion-affected-by-2013-hack/>)), some chose to delete their account for good. The process itself may be easy, but many found that their [accounts would persist](http://www.zdnet.com/article/yahoo-not-deleting-email-accounts-say-users/) (<http://www.zdnet.com/article/yahoo-not-deleting-email-accounts-say-users/>) and wouldn't get wiped.

9. TRUMP USED AN UNSECURED ANDROID PHONE FOR MONTHS INTO HIS PRESIDENCY ([HTTP://WWW.ZDNET.COM/ARTICLE/FOR-NATIONAL-SECURITY-TRUMP-TRADES-IN-PHONE-FOR-SECRET-SERVICE-APPROVED-DEVICE/](http://www.zdnet.com/article/for-national-security-trump-trades-in-phone-for-secret-service-approved-device/))

Even after President Trump took office, he was reportedly still using [his old Galaxy S3 phone](https://www.theverge.com/2017/1/25/14386524/trump-unsecured-android-phone-report) (<https://www.theverge.com/2017/1/25/14386524/trump-unsecured-android-phone-report>) to tweet and take calls. The phone was out-of-date and didn't have the latest patches, unlike newer phones, causing a significant security risk to the commander-in-chief. One report said an [attacker gaining access](http://www.buzzfeed.com/josephbernstein/donald-trumps-twitter-account-is-a-security-disaster-waiting) (<http://www.buzzfeed.com/josephbernstein/donald-trumps-twitter-account-is-a-security-disaster-waiting>) to Trump's phone -- and his Twitter account -- could be a "security disaster waiting to happen." He was since [given a more secure smartphone](http://www.zdnet.com/article/for-national-security-trump-trades-in-phone-for-secret-service-approved-device/) (<http://www.zdnet.com/article/for-national-security-trump-trades-in-phone-for-secret-service-approved-device/>).

10. NOBODY SEEMS TO KNOW WHAT RUDY GIULIANI'S CYBERSECURITY FIRM ACTUALLY DOES

([HTTP://WWW.ZDNET.COM/ARTICLE/NOBODY-SEEMS-TO-KNOW-WHAT-RUDY-GIULIANIS-CYBERSECURITY-COMPANY-ACTUALLY-DOES/](http://www.zdnet.com/article/nobody-seems-to-know-what-rudy-giulianis-cybersecurity-company-actually-does/))

The former New York mayor has been advising Trump's administration on cybersecurity, largely in part due to owning his own private cybersecurity company. But nobody seems to know exactly what his company does, and the mystery remains. What isn't a secret is [how horribly insecure his company's website is](https://gizmodo.com/the-website-of-donald-trumps-top-cyber-security-advisor-1791145791) (<https://gizmodo.com/the-website-of-donald-trumps-top-cyber-security-advisor-1791145791>). Not a good look.

These were 2017's biggest hacks, leaks, and... (</pictures/biggest-hacks-leaks-and-data-breaches-2017/>)

[SEE FULL GALLERY \(/pictures/biggest-hacks-leaks-and-data-breaches-2017/\)](/pictures/biggest-hacks-leaks-and-data-breaches-2017/)



</pictures/biggest->



</pictures/biggest->



</pictures/biggest->



</pictures/biggest->



</pictures/biggest->

</pictures/biggest->
[hacks-leaks-and-data-](/pictures/biggest-)
[breaches-2017/6/](/pictures/biggest-)

</pictures/biggest->

[...](#)

1 - 5 of 28

[NEXT >](#)

Contact me securely (<https://medium.com/@zackwhittaker/how-to-contact-me-securely-38dc5c5bc756>)

Zack Whittaker can be reached securely on Signal and WhatsApp at 646-755-8849, and his PGP fingerprint for email is: 4DoE 92F2 E36A EC51 DAAE 5D97 CB8C 15FA EB6C EEA5.

Read More (<https://medium.com/@zackwhittaker/how-to-contact-me-securely-38dc5c5bc756>)

ZDNET INVESTIGATIONS

Lawsuits threaten infosec research — just when we need it most (<http://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/>)

NSA's Ragtime program targets Americans, leaked files show (<http://www.zdnet.com/article/ragtime-program-appear-in-nsa-leaked-files/>)

Leaked TSA documents reveal New York airport's wave of security lapses (<http://www.zdnet.com/article/leaked-files-reveal-catalog-of-airport-security-lapses/>)

US government pushed tech firms to hand over source code (<http://www.zdnet.com/article/us-government-pushed-tech-firms-to-hand-over-source-code/>)

Millions of Verizon customer records exposed in security lapse (<http://www.zdnet.com/article/millions-verizon-customer-records-israeli-data/>)

Meet the shadowy tech brokers that deliver your data to the NSA (<http://www.zdnet.com/article/meet-the-shadowy-tech-brokers-that-deliver-your-data-to-the-nsa/>)

Inside the global terror watchlist that secretly shadows millions (<http://www.zdnet.com/article/inside-the-global-terrorism-blacklist-secretly-shadowing-millions-of-suspects/>)

FCC chairman voted to sell your browsing history — so we asked to see his (<http://www.zdnet.com/article/fcc-chairman-browsing-history-freedom-of-information/>)

198 million Americans hit by 'largest ever' voter records leak (<http://www.zdnet.com/article/security-lapse-exposes-198-million-united-states-voter-records/>)

Britain has passed the 'most extreme surveillance law ever passed in a democracy' (<http://www.zdnet.com/article/snoopers-charter-expansive-new-spying-powers-becomes-law/>)

Microsoft says 'no known ransomware' runs on Windows 10 S — so we tried to hack it (<http://www.zdnet.com/article/microsoft-no-known-ransomware-windows-we-tried-to-hack-it/>)

Leaked document reveals UK plans for wider internet surveillance (<http://www.zdnet.com/article/leaked-document-reveals-uk-plans-for-wider-internet-surveillance/>)

RELATED TOPICS:

SECURITY TV

DATA MANAGEMENT

CXO

DATA CENTERS

[LOG IN TO COMMENT](#)

| [Community Guidelines](#)

[Join Discussion](#)

[ADD YOUR COMMENT](#)